## AMENDMENTS TO THE SPECIFICATION

On page 7, paragraph **[0017]**, please amend as follows:

**[0017]** Various embodiments of the present invention may be provided as a computer program product, which may include a machine-readable medium having stored thereon instructions, which may be used to program a computer (or other electronic devices) to perform a process according to various embodiments of the present invention. ~~The machine-readable medium may include, but is not limited to, floppy diskettes, optical disks, CD-ROMs, magneto-optical disks, ROMs, RAMs, EPROMs, EEPROMs, magnetic or optical cards, flash memory, or another type of media/machine-readable medium suitable for storing electronic instructions.~~ The machine-readable medium may include, but is not limited to, a floppy diskette, an optical disk, a Compact Disk-Read Only Memory (CD-ROM), a magneto-optical disk, a Read Only Memory (ROM), a Random Access Memory (RAM), an Erasable Programmable ROM (EPROM), an Electrically EPROM (EEPROM), a magnetic or optical card, a flash memory, or another type of media/machine-readable medium suitable for storing electronic instructions. Moreover, various embodiments of the present invention may also be downloaded as a computer program product, wherein the program may be transferred from a remote computer to a requesting computer by way of data signals embodied in a carrier wave or other propagation medium via a communication link (e.g., a modem or network connection).

On pages 8 and 9, paragraphs **[0021]** and **[0022]**, please amend as follows:

**[0021]** System 100 may include a dynamic storage device, referred to as main memory 116, or a ~~random access memory (RAM)~~RAM or other memory devices coupled to the processor bus 112 for storing information and instructions to be executed by the processors 102-106. Main memory 116 also may be used for storing temporary variables or other intermediate information during execution of instructions by the processors 102-106. System 100 may include a read only memory (ROM) and/or other static storage device coupled to the processor bus 112 for storing static information and instructions for processors ~~110~~102-106.

**[0023]** Main memory 116 or dynamic storage device may include a magnetic disk or an optical disc for storing information and instructions. I/O device 130 may include a display device (not shown), such as a cathode ray tube (CRT) or Liquid Crystal Display (LCD), for displaying information to an end user. For example, graphical and/or textual indications of installation status, time remaining in the trial period, and other information may be presented to the prospective purchaser on the display device. I/O device 130 may also include an input device (not shown), such as an alphanumeric input device, including alphanumeric and other keys for communicating information and/or command selections to processors ~~110~~102-106. Another type of user input device includes cursor control, such as a mouse, a trackball, or cursor direction keys for communicating direction information and command selections to the processors 102-106 and for controlling cursor movement on the display device.

On page 10, paragraph **[0026]**, please amend as follows:

**[0026]** **Figure 2** is a block diagram illustrating an embodiment of a hardware Trusted Computing Base. As illustrated, computer system or device (system) 100 may include a hardware Trusted Computing Base (TCB) 206 based on a hardware device, such as a Trusted Platform Module (TPM) 204, a processor 102 having security extensions to provide a tamper-resistant facility for software measurement and address space isolation, and a system interface or chipset, such as the security-enhanced chipset[[,]] 114 to provide special security capabilities including the ability to selectively protect main memory 116 from, for example, Direct Memory Access (DMA)-based input/output (I/O). The system 100 may be referred to as the TCB-based system 100.

On page 11, paragraph **[0028]**, please amend as follows:

**[0028]** According to one embodiment, the processor 102 may be used to measure the booted software in a tamper-resistant manner, and the TPM 204 may be utilized as a secure co-processor to provide tamper-resistant secure storage for confidential information, tamper-resistant storage for measured values, and tamper-resistant cryptographic algorithms to support attestation protocols. For example, the tamper-resistant processor 102 may be used to measure software that may be loaded on the system 100. According to one embodiment, the measured value may be a cryptographic hash of the software image and may represent the integrity of the measured software. According to one embodiment, the measured value may be subsequently signed by a tamper-resistant co-processor (e.g., the TPM 204) using a key that may be contained and hidden in the TCB 206 and more particularly, for example, in the TPM 204. According

to one embodiment, the process of attestation may be used for having the signed value reported to a remote system via, for example, a cryptographic protocol. The remote system may ascertain the trustworthiness of the measured software and may make a trust decision based on the trustworthiness of information reported by the hardware TCB 206 of the measured system 100.

On page 20, paragraph **[0049]**, please amend as follows:

**[0049] Figure 5** is a block diagram illustrating an embodiment of a horizontally extended Trusted Computing Base. According to one embodiment, as described with ~~referenced~~ reference to Figures 2 and 3, a Trusted Platform Module (TPM) 204 and other trustworthy hardware components (e.g., hardware-based measurement of booted software and Direct Memory Access (DMA) protection from input/output (I/O) devices) may be used to form a trustworthy hardware computing base, such as Level one tamper-resistant hardware Trusted Computing Base (L1 TCB) 206. According to one embodiment, the L1 TCB 206 may be extended horizontally into a horizontally extended TCB 500.

On page 23, paragraph **[0053]**, please amend as follows:

**[0053]** According to one embodiment, the software-based L2 TCB 502 may not merely virtualize the functionality of the hardware-based L1 TCB 206, but also perform the virtualization such that the trust and security properties of the hardware-based L1 TCB 206 may be mimicked or imitated in software of the L2 TCB 502. According to one embodiment, the mimicking of the trust and security properties of the L1 TCB 206 may be necessary for a software TCB layer, such as the L2 TCB 502, to represent its own

trustworthiness to a third party, such as a remote entity or system, with a need to know. According to one embodiment, the virtual TPMs 504-506, having the trust and security properties of the hardware TPM 204 of the L1 TCB 206, may facilitate a secured and measured launch of software in the virtual containers 508-510 [[to]] so that the launched software within the virtual containers 508-510 may fail to recognize that the virtual containers 508-510 are not running directly in contact with the L1 TCB 206.